CLAIMS

What is claimed is:

1. A system for generating, installing to a plurality of linked remote computers, and monitoring a secure network of nodes, said system comprising:

A. at least one software application;

B. an installation server, configured to facilitate installation of said at least one software application;

C. a generator, configured to generate a plurality of software components from a network definition, including a plurality of agent modules, wherein each agent module is executable on a corresponding remote computer to initiate communication with said installation server and subsequent installation of a corresponding software application on said remote computer to form a node, wherein each of said nodes is capable of automatically establishing communication with others of said nodes according to said network definition; and

D. a monitor node configured to monitor security of said network.

2. A system according to claim 1, wherein the remote computers are linked substantially by the Internet.

3. A system according to claim 1, wherein the remote computers are linked substantially by an intranet.

4. A system according to claim 1, wherein said network definition includes a plurality of node definitions, each node definition including:

C. (i) an identification of one of said plurality of remote computers;

(ii) an identification of at least one software application to be installed on said remote computer to form a node; and

(iii) an identification of each other node to which said node is to be linked.

5. A system according to claim 4, wherein said identification of each of said plurality remote computers includes:

C. (i) (a) an IP address; and

(b) a node name.

6. A system according to claim 1, wherein said plurality of software components further includes:

C. (i) a plurality of node configuration files, wherein a different one of said node configuration files corresponds to a different node and includes information for facilitating selective communication with others of said nodes according to said network definition; and

(ii) at least one network information file, having information corresponding to substantially all links between nodes and accessible by said monitor node to facilitate the selective linking of said nodes.

7. A system according to claim 1, wherein said installation server is configured to facilitate said installation of said corresponding software application as a function of a verification that said agent module is executing on said corresponding remote computer, according to said network definition.

8. A system according to claim 1, wherein said installation server is configured to facilitate said installation of said corresponding software application as a function of a verification that said agent module has not been previously installed.

9. A system according to claim 1, further including a second monitor node configured to determine the presence of an interposed, unintended node.

10. A system according to claim 1, wherein said monitor node is further configured to selectively terminate operation and connection of one or more tainted nodes in response to a detected security violation.

11. A system according to claim 10, wherein said installation server is further configured to initiate a regeneration of a set of said software components, reinstallation of said at least one software application, and selective relinking to other nodes for each of said selectively terminated one or more tainted nodes and according to said network definition.

12. A system according to claim 1, wherein said monitor node and each of said nodes communicate using secure data transfer.

13. A system according to claim 12, wherein said secure data transfer is accomplished using data encryption, and wherein data transferred in each direction between two linked nodes is encrypted differently.

14. A system according to claim 13, wherein each of two linked nodes uses a unique pair of encryption keys to accomplish said data encryption, and each pair of encryption keys includes a substantially hidden private key and a public key.

15. A system according to claim 14, wherein said monitor node is further configured to selectively initiate a coordinated strobing of each pair encryption keys between two linked nodes.

16. A system according to claim 1, further including:

E. an account server, configured to generate billing information as a function of the selective linking of said node to said other nodes.

17. A system according to claim 1, wherein said installation server is configured to communicate with each of said plurality of remote computers using data encryption.

18. A system according to claim 17, wherein said installation uses a randomly generated private key and public key pair for data encryption, wherein data to be transferred to said installation server is encrypted using said public key and is decrypted by said installation server using said private key.

19. A system according to claim 18, further including:

E. a second monitor node, configured to compare the installation server public key with the encryption key used by one of said plurality of remote computers to encrypt data sent to said installation server, a negative comparison being indicative of a security violation.

20. A system for generating, installing to a plurality of linked remote computers, and monitoring a secure network of nodes, said system comprising:

A. at least one software application;

B. an installation server, configured to facilitate installation of said at least one software application;

C. a generator, configured to generate a plurality of software components from a network definition, including a plurality of agent modules, wherein each agent module is executable on a corresponding remote computer to initiate communication with said installation server and subsequent installation of a corresponding software application on said remote computer to form a node,

wherein each of said nodes is capable of automatically establishing communications with others of said nodes according to said network definition; and

D. a monitor node configured to monitor security of said network, wherein said monitor node and each of said nodes communicate using secure data transfer.

21. A system according to claim 20, wherein said secure data transfer is data encryption and each of two linked nodes uses a unique set of encryption keys to accomplish said data encryption.

22. A system according to claim 21, wherein said encryption keys are substantially randomly generated.

23. A system according to claim 21, wherein each set of said encryption keys includes a hidden private key and a public key, and said public key is used by a first node in a link to encrypt data transmitted to a second node in the link, and said private key is used to decrypt said data by said second node.

24. A system according to claim 21 wherein said monitor node is further configured to selectively initiate a coordinated strobing of each set of encryption keys between two linked nodes.

25. A system according to claim 21, wherein said monitor node is further configured to effectuate persistence of said encryption keys, and wherein when a first set of encryption keys used by two linked nodes is strobed, a second set of encryption keys is randomly generated, and said first and said second sets are stored in a memory, such that when one or both of said two linked nodes loses its connection with the other of said two linked nodes , said two linked nodes attempt to reestablish said connection alternatively using said first and said second set of encryption keys.

26. A system according to claim 21, wherein said installation server is configured to communicate with each of said plurality of remote computers using data encryption.

27. A system according to claim 26, wherein said installation uses a randomly generated private key and public key pair for data encryption, wherein data to be transferred to said installation server is encrypted using said public key and is decrypted by said installation server using said private key.

28. A system according to claim 27, further including:

E. a second monitor node, configured to compare the installation server public key with the encryption key used by one of said plurality of remote computers to encrypt data sent to said installation server, a negative comparison being indicative of a security violation.

29. A system for generating, installing to a plurality of linked remote computers, and monitoring an auditible secure network of nodes, said system comprising an secure network:

A. at least one software application;

B. an installation server, configured to facilitate installation of said at least one software application;

C. a generator, configured to generate a plurality of software components from a network definition, including a plurality of agent modules, wherein each agent module is executable on a predetermined corresponding remote computer to initiate communication with said installation server and subsequent installation of a predetermined corresponding software application on said remote computer to form a node, wherein each of said nodes is capable of automatically establishing communication with others of said nodes according to said network definition, and wherein said subsequent installation is contingent upon a first verification that said agent module is installed on its corresponding remote computer and wherein said installation is further contingent upon a second verification that said software application is installed on its predetermined corresponding remote computer; and

D. a monitor node configured to monitor security of said network.

30. A system according to claim 29, wherein said installation server is configured to terminate said installation of said at least one software application on said corresponding remote computer if said agent module has been previously installed.

31. A system according to claim 29, wherein said installation server is configured to terminate said installation of said at least one software application on said corresponding remote computer if said agent module is not installed on said corresponding computer.

32. A system according to claim 29 wherein said installation server is configured to perform said subsequent installation in response to receipt of a password entered at said remote computer, as said first verification.

33. A system according to claim 29, wherein said installation server is configured to complete said installation in response to receipt of a password entered at said remote computer, as said second verification.

34. A system according to claim 29, further including:

E. a software component analyzer, configured to analyze said software components and determine the presence of trap doors.

35. A system according to claim 29, wherein said installation server is configured to communicate with each of said plurality of remote computers using data encryption.

36. A system according to claim 35, wherein said installation uses a randomly generated private key and public key pair for data encryption, wherein data to be transferred to said

installation server is encrypted using said public key and is decrypted by said installation server using said private key.

37. A system according to claim 36, further including:

E. a second monitor node, configured to compare the installation server public key with the encryption key used by one of said plurality of remote computers to encrypt data sent to said installation server, a negative comparison being indicative of a security violation.

38. A method for generating, installing to a plurality of remote computers, and monitoring a secure network having a plurality of nodes, a generator, an installation server, and a monitor node, the method comprising the steps:

A. creating a network definition, including information that describes each remote computer, at least one software application to be installed on each remote computer, and each link between nodes;

B. generating with said generator a plurality of software components, as a function of said network definition, including a plurality of agent modules, wherein each agent module is executable on a preselected one of said remote computers and includes functionality to communicate with said installation server;

C. executing an agent module on its corresponding remote computer, wherein said agent module automatically establishes communication with said installation server;

D. downloading, using said installation server, to said remote computer a corresponding at least one software application;

E. executing said at least one software application on said remote computer to form a node and automatically establishing a connection with said monitor node;

F. selectively linking said node to others of said plurality of nodes according to said network definition; and

G. repeating steps C through F for each agent module and corresponding remote computer.

39. The method of claim 38, wherein step A includes identifying each remote computer by an IP address and a node name.

40. The method of claim 38 wherein step B further includes generating:

(i) a plurality of node configuration files, wherein each node configuration file corresponds to one of said nodes; and

(ii) a set of network information files, including information corresponding to a plurality of links required to form said network.

41. The method of claim 38 wherein step D further includes verifying that said agent module is executing on a corresponding remote computer, according to said network definition, as a prerequisite to downloading said at least one software application.

42. The method of claim 41 wherein step B includes generating a unique local password for each node and said verifying in step D includes:

(i) entering said local password at said remote computer; and

(ii) verifying said local password at said installation server.

43. The method of claim 38 wherein step D further includes verifying that said agent module has not been previously installed, as a prerequisite to downloading said at least one software application.

44. The method of claim 38 wherein step F further includes verifying that said software application is executing on its corresponding remote computer according to said network definition, as a prerequisite of selectively linking said node to others of said plurality of nodes.

45. The method of claim 44 wherein step B includes generating a unique audit password for each node and said verification in step F includes:

(i) entering said audit password at said remote computer; and

(ii) verifying said audit password.

46. The method of claim 38, further including a step:

H. terminating operation and connection of one or more tainted nodes, under control of said monitor node, in response to detection of a security violation related to

said tainted node.

47. The method of claim 46, further including a step:

I. repeating steps B-G for each of said one or more tainted nodes.

48. The method of claim 38, wherein step B further includes generating for each node in a pair of linked nodes, a set of encryption keys, including a private key and a public key, to facilitate secure communication between said linked nodes.

49. The method of claim 48, further including step:

H. (i) selecting said pair of linked nodes; and

(ii) strobing each set of encryption keys for said linked nodes.

50. The method of claim 49, wherein said two linked nodes are a first node and a second node and said strobing includes the steps:

(a) ceasing data transfer between said first and second nodes;

(b) randomly generating a new first private key for said first node;

(c) deriving a new first public key from said new first private key and storing said new first private and public keys;

(d) encrypting said new first public key with a current second public key of said second node and transmitting said new first public key to said second node;

(e) decrypting with a current second private key said new first public key and storing said new first public key at said second node and randomly generating a new second private key;

(f) deriving a new second public key from said new second private key and storing said new second private and public keys;

(h) encrypting said new second public key with a current first public key of said first node and transmitting said new second public key to said first node;

(i) decrypting with a current first private key said new second public key and storing said new second public key at said first node;

(j) exchanging confirmations between said first and second nodes to use said new first and second private and public keys; and

(k) resuming data transfer between said two linked nodes.

51. The method of claim 50, wherein each pair of linked nodes also uses at least one session key to encrypt data transferred between said linked nodes and said strobing further includes:

randomly generating, exchanging and storing at least one new session key for said linked nodes, between steps H(ii)(a) and H(ii)(k).

52. The method of claim 50 wherein said strobing is strobing with persistence and said step H(ii) further includes saving said current first and second public and private keys.

53. The method of claim 38, wherein said network further includes an account server, said method further comprising the step of:

H. (i) communicating to said account server said linking of said node, in step F; and

(ii) generating billing information related to said linking of said node.

54. The method of claim 38, wherein step B includes generating a unique set of encryption keys for each node and said monitor node.

55. The method of claim 54, wherein step E includes the steps of:

(i) logging into said monitor node by said node using a unique encryption key from a corresponding set of node encryption keys generated by said generator; and

(ii) logging into said node using a unique monitor node encryption key from a corresponding set of monitor node encryption keys generated by said generator.

56. The method of claim 38, wherein said secure network further includes a second monitor node and said installation server communicates with each of said plurality of remote computers using a private and public encryption key pair, the method further including the step of:

H. (i) comparing the public key of said installation server with a key used by one of said plurality of remote computers to encrypt data sent to said installation server; and

(ii) issuing a security violation message, in the event of a negative comparison.

57. A method for generating, installing to a plurality of remote computers, and monitoring a secure network having a plurality of nodes, a generator, an installation server, and a monitor node, said network used for conducting financially related transactions between a custody system of a bank and a trading system of a financial client, the method comprising the steps of:

A. creating, by a bank sales department, a network definition embodying the network required by the financial client and to be generated, installed and monitored by the bank;

B. modeling and testing said network definition, by a bank development group;

C. obtaining authorization from a bank network administration group and installing said network definition on said generator, by said bank development group;

D. obtaining by said bank sales group a sales password and authorization to install network from said network administration group;

E. auditing on said generator a generated network definition by comparing said generated network definition to said network definition and inputting said sales password as an indication of a favorable comparison, by said bank sales group;

F. obtaining by a bank audit group, an audit password and authorization to install network from said network administration group;

G. auditing on said generator a generated network definition by comparing said

generated network definition to said network definition and inputting said audit password as an indication of a favorable comparison, by said bank audit group;

H. generating with said generator a plurality of software components to be installed on said plurality of remote computers to form said plurality of nodes of said network, said components including:

(i) a plurality of agent modules, each agent module having the capability to establish communications with said installation server;

(ii) a local sales password, for each agent module;

(iii) a local audit password for each agent module;

I. registering said agent modules with said installation server, wherein said installation server has access to at least one or more bank custody software applications to be stored on each of said plurality of remote computers to form said nodes, according to said network definition;

J. communicating to each remote computer a corresponding one of said local sales passwords to a sales department representative;

K. communicating to each remote computer a corresponding one of said local audit passwords to an audit department representative;

L. executing each agent module on its corresponding remote computer, entering said local sales password to verify that said agent module is installed on its corresponding remote computer according to said network definition, and downloading said corresponding at least one bank custody software application;

M. executing each of said at least one software applications on its corresponding

remote computer, establishing communication with said monitor node, entering said local audit password to verify that said at least one software application is installed on its corresponding remote computer according to said network definition; and

N. selectively linking said nodes into said network.

58. A method for generating, installing to a plurality of remote computers, and monitoring a secure network having a plurality of nodes, a generator, an installation server, and a monitor node, wherein the secure network is used for the exchange of confidential data between a first system of a first group and a second system of a second group, the method comprising the steps:

A. creating a network definition, including information that describes each remote computer, at least one first group software application to be installed on each remote computer, and each link between nodes;

B. generating with said generator a plurality of software components, as a function of said network definition, including a plurality of agent modules, wherein each agent module is executable on a preselected one of said remote computers and includes functionality to communicate with said installation server;

C. executing an agent module on its corresponding remote computer, wherein said agent module automatically establishes communication with said installation server;

D. (i) human auditing and verifying that said agent module is installed on its

corresponding remote computer according to said network definition by a third group; and

(ii) downloading, using said installation server, to said remote computer a corresponding at least one first group software application;

E. (i) executing said at least one first group software application on said remote computer to form a node and automatically establishing a connection with said monitor node; and

(ii) human auditing and verifying that said at least one first group software application is installed on its corresponding remote computer according to said network definition by a fourth group, independent from said third group;

F. communicating with others of said plurality of nodes according to said network definition; and

G. repeating steps C through F for each agent module and corresponding remote computer.

59. The method of claim 58 wherein said confidential data is financial data and said first system of said first group is a custody system of a bank and said second system of said second group is a trading system of a financial services group.